Brittany Resch (*pro hac vice*)
Raina C. Borrelli (*pro hac vice*)
STRAUSS BORRELLI PLLC
One Magnificent Mile
980 N Michigan Avenue, Suite 1610
Chicago Illinois, 60611
T: (872) 263-1100
F: (872) 263-1109
bresch@straussborrelli.com
raina@straussborrelli.com

Andrew W. Ferich (*pro hac vice*)
AHDOOT & WOLFSON, PC
201 King of Prussia Road, Suite 650
Radnor, PA 19087
T.: 310.474.9111
F: 310.474.8585
aferich@ahdootwolfson.com

Anthony L. Parkhill (*pro hac vice*)
BARNOW AND ASSOCIATES, P.C.
205 West Randolph Street, Ste. 1630
Chicago, IL 60606
T.: 312.621.2000
F: 312.641.5504
aparkhill@barnowlaw.com

Counsel for Plaintiffs
[Additional Counsel Appear on Signature Page]

UNITED STATES DISTRICT COURT
DISTRICT OF UTAH

LAZARO STERN, CELESTE ALLEN, LISA KUCHERRY, PETER SMITH, and SHARON THOMPSON, individually and on behalf of all others similarly situated, Plaintiffs, v. ACADEMY MORTGAGE CORPORATION, Defendant.	Case No. 2:24-cv-00015-DBB-DAO Judge David B. Barlow Magistrate Judge Daphne A. Oberg **PLAINTIFFS' MEMORANDUM OF LAW IN OPPOSITION TO DEFENDANT'S MOTION TO DISMISS**

I. INTRODUCTION

On March 21, 2023, Defendant Academy Mortgage Corporation ("Defendant" or "Academy") experienced a data breach (the "Data Breach") that exposed the personally identifying information ("PII") of 284,443 of its current and former employees and customers (the "Class" or "Class Members"). As a result of the Data Breach, Peter Smith, Celeste Allen, Lazaro Stern, Lisa Kucherry, and Sharon Thompson (collectively, "Plaintiffs") and Class Members now face the substantial risk of imminent identity theft and fraud—some of which has already occurred. To make matters worse, the notorious cybercriminal group "ALPHV BlackCat" claimed credit for the Data Breach—and promised to leak the stolen PII on the dark web. Plaintiffs brought this litigation as a class action to seek remedies for themselves and other Class Members for the injuries caused by Academy's misconduct.

Academy attempts to sidestep responsibility for its Data Breach, asserting that Plaintiffs' claims should be dismissed under Rule 12(b)(1) and 12(b)(6). Academy's arguments are unavailing. Plaintiffs sufficiently state numerous injuries-in-fact, each of which is enough, by itself, to satisfy Plaintiffs' pleading burden. Further, Academy's misconduct gives rise to the claims alleged, which Plaintiffs have sufficiently pleaded at this early stage. As discussed in detail below, the motion to dismiss should be denied in its entirety.

II. FACTUAL BACKGROUND

A. Academy Collects the PII of Plaintiffs and the Class

Academy is an independent mortgage lender based in Draper, Utah. Doc. 41, ("Compl."), ¶2. It collects and maintains the PII—including first names, last names, dates of birth, addresses, email addresses, phone numbers, credit information, financial information, and Social Security numbers ("SSN")—of its current and former employees and customers. *Id*. ¶¶1, 90. In doing so,

Academy agrees to safeguard the PII within its custody and control. *Id*. ¶91. Indeed, in its "Privacy Policy" Academy promises that it is "committed to ensuring that your information is secure" and that it "protects data using administrative, technical, and physical safeguards[.]" *Id*. ¶92. It also promises that it "use[s] commercially reasonable efforts to protect your [PII] . . . from access, loss, misuse, alteration, or destruction by any unauthorized party." *Id*.

B. The Data Breach, ALPHV BlackCat, and the Dark Web

Despite its promises, Academy breached its duties and failed to use reasonable data security—thereby leaving Plaintiffs' and Class Members' PII as "low hanging fruit" for cybercriminals. *Id*. ¶93. On or about March 21, 2023, Academy discovered the Data Breach. *Id*. ¶97. Academy admitted that "an unauthorized third party accessed and disabled some of our systems." *Id*. ¶98.[1] As a result, Academy exposed PII for 284,443 Class Members, including at least first names, last names, and SSNs. *Id*. ¶¶98, 102. Despite the severity of the Data Breach, Academy failed to warn Class Members in a timely manner, delaying notice until December 20, 2023—274 days after discovering the Data Breach. *Id*. ¶98.

The notorious cybercriminal group "ALPHV BlackCat" took credit for the Data Breach, claiming that it was "in [Academy's] network for a very long time[.]" *Id*. ¶¶103–07. Thereafter, ALPHV BlackCat promised to leak the stolen PII on the dark web—meaning that Plaintiffs and Class Members now face an imminent risk of further identity theft and fraud. *Id*. Indeed, a report by the federal Cybersecurity & Infrastructure Security Agency ("CISA") suggests that ALPHV

[1]Academy has not publicly disclosed when ALPHV BlackCat first gained access to its data security systems, and it is unknown how long the cybercriminals had unfettered access to Academy's systems and the PII thereon. Compl. ¶¶4, 97. Given that the hackers were able to disable portions of Academy's systems, it is likely that the length of the intrusion was substantial. *Id*. ¶106.

BlackCat will—and seemingly did—disseminate the stolen PII on the dark web for other cybercriminals to buy, access, and download. *Id*.

C. Plaintiffs' Experiences and Injuries Due to the Data Breach

As a precondition of receiving employment or financial services, Plaintiffs entrusted their sensitive PII to Academy. *Id*. ¶¶24, 37, 49, 61, 73. They would not have disclosed their PII had they known that Academy's data security was inadequate. *Id*. Following (and as a result of) the Data Breach, Plaintiffs suffered numerous injuries—including identity theft and fraud, increased risk of future harm, lost time, emotional injuries, influx of scam calls and messages (e.g., "text messages related to taking out lines of credit" and "spam calls, up to ten a day"), and property damage to their PII. *Id*. ¶¶28–32, 39–44, 51–56, 63–68, 90, 97, 165.

III. LEGAL STANDARD

Under Rule 12(b)(6), plaintiffs need only "state a claim to relief that is plausible on its face." *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007). While allegations must "raise a right to relief above the speculative level," detailed allegations are not required. *Id*. at 555. A claim is plausible when the facts allow the court to draw the reasonable inference that the defendant is liable for the alleged conduct. *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009). And "[a]ll well-pleaded facts . . . must be taken as true, and the court must liberally construe the pleadings and make all reasonable inferences in favor of the non-moving party." *Brokers' Choice of Am., Inc. v. NBC Universal, Inc*., 861 F.3d 1081, 1105 (10th Cir. 2017) (internal quotation marks omitted).

A Rule 12(b)(1) motion challenges the Court's subject matter jurisdiction. *Baker v. USD 229 Blue Valley*, 979 F.3d 866, 872 (10th Cir. 2020). When a defendant brings a facial attack, the court "assumes the allegations in the complaint are true[.]" *Id*. (citing *Pueblo of Jemez v. United States*, 790 F.3d 1143, 1148 n.4 (10th Cir. 2015)).

IV. ARGUMENT

A. Plaintiffs Established Article III Standing.

Article III standing requires that a plaintiff "(1) suffered an injury in fact, (2) that is fairly traceable to the challenged conduct of the defendant, and (3) that is likely to be redressed by a favorable judicial decision." *Spokeo, Inc. v. Robins*, 578 U.S. 330, 338 (2016). Additionally, an injury-in-fact must be "concrete, particularized, and actual or imminent[.]" *TransUnion LLC v. Ramirez*, 594 U.S. 413, 423 (2021). Concrete harms include "traditional tangible harms[] such as physical harms and monetary harms" but also "injuries with a close relationship to harms traditionally recognized" such as "reputational harms, disclosure of private information, and intrusion upon seclusion." *Id*. at 424–25.

The "risk of future harm" can be a concrete injury-in-fact. *Id*. at 435 (citing *Clapper v. Amnesty Int'l USA*, 568 U.S. 398, 414 n.5 (2013)). Indeed, the risk of future harm provides standing for "injunctive relief to prevent the harm from occurring . . . so long as the risk of harm is sufficiently imminent and substantial." *Id*. However, in a suit for damages, the risk of future harm is concrete only if plaintiffs "were independently harmed by their exposure to the risk itself—that is, that they suffered some other injury[.]" *Id*. at 437. The Supreme Court suggested that an "emotional injury" could satisfy the "some other injury" requirement. *Id*. at 436–37, n.7.

Plaintiffs' allegations establish Article III standing. After all, Plaintiffs need not establish standing on every theory of injury-in-fact. In other words, dismissal is proper only if every theory of injury-in-fact is implausible. *See Webb v. Injured Workers Pharmacy, LLC*, 72 F.4th 365, 375 (1st Cir. 2023) (explaining that a different theory of injury "provides an independent basis for . . . standing"); *Bohnak v. Marsh & McLennan Cos*., 79 F.4th 276, 286 (2d Cir. 2023) ("separate and concrete harms . . . independently support standing").

1. Increased Risk of Identity Theft & Fraud

All Plaintiffs suffer from the substantial risk of identity theft and fraud, establishing Article III standing for all class members. *Gordon v. Chipotle Mexican Grill, Inc*., 344 F. Supp. 3d 1231, 1241 (D. Colo. 2018) (plaintiffs "demonstrate[] a cognizable Art. III injury, based on the risk of exposure to future fraudulent purchases or identity theft") (quoting *Engl v. Nat. Grocers by Vitamin Cottage, Inc*., No. 15-cv-02129, 2016 U.S. Dist. LEXIS 187733, at *19 (D. Colo. Sept. 21, 2016) (unpublished)); *Maser v. Commonspirit Health*, No. 1:23-cv-01073, 2024 U.S. Dist. LEXIS 102196, at *9 (D. Colo. Apr. 16, 2024) (unpublished) ("[a]n allegation of future injury may suffice [as a concrete harm] if the threatened injury is certainly impending, or there is a substantial risk that the harm will occur[.]") (quoting *Susan B. Anthony List v. Driehaus*, 573 U.S. 149, 158 (2014)).[2]

2. Identity Theft & Fraud

Moreover, the Complaint alleges actual misuse of PII (e.g., the fraudulent loan for $9,225) which conclusively establishes Article III standing for all class members because the increased risk of theft and fraud has ***already*** materialized into a concrete injury. Compl. ¶65; *Gordon*, 344 F. Supp. 3d at 1241 (finding Article III standing when plaintiff alleged identity theft and fraud); *Hapka v. CareCentrix, Inc*., No. 16-2372, 2016 U.S. Dist. LEXIS 175346, at *6 (D. Kan. Dec. 19, 2016) (unpublished) (same); *F.S. v. Captify Health, Inc*., No. 23-1142, 2024 U.S. Dist. LEXIS

[2] Several courts have found that plaintiffs established Article III standing by alleging that they faced a "'substantial risk' that harm will occur" following a data breach, "which may prompt [them] to reasonably incur charges to mitigate or avoid that harm." *Clapper,* 568 U.S. at 414 n.5; *see also In re Zappos.com*, *Inc*., 888 F.3d 1020, 1029 (9th Cir. 2018) ("Plaintiffs have sufficiently alleged an injury in fact based on a substantial risk that the Zappos hackers will commit identity fraud or identity theft."); *Remijas v. Neiman Marcus Group, LLC*, 794 F.3d 688, 693 (7th Cir. 2015) ("customers should not have to wait until hackers commit identity theft or credit-card fraud in order to give the class standing, because there is an 'objectively reasonable likelihood' that such an injury will occur") (internal citation omitted).

53711, at *8 (D. Kan. Mar. 26, 2024) (unpublished) ("Misuse of plaintiff's data could cause concrete, present injury—i.e., fraudulent charges[.]"). Notably, Academy has not even contested this point. *See* Doc. 49, 2 n.1, 12. Moreover, such identity theft is plainly traceable to Academy's Data Breach because the "disclosure of social security numbers, birth dates, and names is more likely to create a risk of identity theft or fraud." *Maser*, 2024 U.S. Dist. LEXIS 102196, at *12.

Plaintiffs' allegations of actual misuse are significant because within the Tenth Circuit, allegations of the "misuse of the comprised data is an important inflection point that explains many of the differing results." *Captify*, 2024 U.S. Dist. LEXIS 53711, at *7 (collecting cases). While the Tenth Circuit has not directly addressed the issue, *see id.*, courts within the Tenth Circuit have "predict[ed] that the Tenth Circuit . . . would follow the line of cases where outcome depends on whether plaintiffs have alleged misuse of their data," *C.C. v. Med-Data Inc*., No. 21-2301, 2022 U.S. Dist. LEXIS 60555, at *11 (D. Kan. Mar. 31, 2022) (unpublished).

Academy broadly misapplies *TransUnion* to argue that Plaintiffs cannot "ride the coattails" of one Plaintiff's allegations of misuse. Doc 49, at 12. To be sure, Plaintiffs acknowledge that "[e]very class member must have Article III standing in order to recover individual damages." *TransUnion*, 594 U.S. at 431. And all class members do by virtue of their increased risk of identity theft and fraud because of Academy's Data Breach. However, Academy stretches *TransUnion* past its breaking point and ignores post-*TransUnion* case law, which hold that all plaintiffs have Article III standing so long as at least one plaintiff suffered misuse of their PII (e.g., identity theft and fraud). *See, e.g.*, *Gordon*, 344 F. Supp. 3d at 1241–43 (holding that one plaintiff "sufficiently allege[d] a substantial risk of future injury" because a different plaintiff already suffered identity theft); *Maser*, 2024 U.S. Dist. LEXIS 102196, at *14 (explaining that "cases that involve targeted breaches, fraud-sensitive data, and actual misuse (as to at least one named plaintiff) easily meet

the Article III standing requirement at the pleading phase"); *Captify*, 2024 U.S. Dist. LEXIS 53711, at *8 (collecting cases) ("Misuse also shows 'an increased risk of identity theft or identity fraud' in the future"); *Hapka*, 2016 U.S. Dist. LEXIS 175346, at *6 ("The fact that her stolen information has been used once has a direct impact on the plausibility of future harm."); *In re Equifax Customer Data Sec. Breach Litig*., 999 F.3d 1247, 1262–63 (11th Cir. 2021) (explaining that "[t]he actual identity theft already suffered by some Plaintiffs further demonstrates the risk of identity theft all Plaintiffs face—though actual identity theft is by no means required when there is a sufficient risk of identity theft").

Moreover, the involvement of ALPHV BlackCat and the allegations of dark web exposure provide an independent basis for establishing Article III standing under the theory of "risk of identity theft and fraud." Compl. ¶¶97–107. Indeed, in *Capiau v. Ascendum Mach., Inc*., the plaintiff alleged that "ALPHV Blackcat" had stolen PII in a data breach. No. 3:24-cv-00142, 2024 U.S. Dist. LEXIS 142393, at *2–3, 15 (W.D.N.C. Aug. 9, 2024) (unpublished). Based on that allegation and ALPHV Blackcat's history and modus operandi, the court held that plaintiff "face[d] a 'substantial risk' of actual PII misuse in the future . . . sufficient to confer Article III standing." *Id*. Thus, Plaintiffs have met—and exceeded—their pleading burden.

3. Violation of Privacy Rights

Plaintiffs suffered from the violation of their privacy rights, which establishes injury-in-fact. *See Lupia v. Medicredit, Inc*., 8 F.4th 1184, 1191–93 (10th Cir. 2021) (explaining that "intrusions on a plaintiff's privacy" can establish Article III standing because such injuries "have roots in long-standing common-law tradition"). For example, in *Gadelhak v. AT&T Servs*., Circuit Judge Barret—now Supreme Court Justice Barrett—explained that an "intrusive invasion of privacy" establishes standing because "[t]he common law has long recognized actions at law

against defendants who invaded the private solitude of another[.]" 950 F.3d 458, 462 (7th Cir. 2020). Indeed, *TransUnion* itself recognized that "injuries with a close relationship to harms traditionally recognized as providing a basis for lawsuits in American courts" include the "disclosure of private information[.]" 594 U.S. at 425.

Here, Plaintiffs suffered an invasion of privacy when their private information was (1) exposed in the Data Breach, (2) seized by ALPHV BlackCat, and (3) seemingly leaked on the dark web. Compl. ¶¶97–107. These allegations are sufficient by themselves to establish the standing of all Plaintiffs. *Green-Cooper v. Brinker Int'l, Inc*., 73 F.4th 883, 890 (11th Cir. 2023) (holding that publication of PII on the dark web "is a concrete injury that is sufficient to establish Article III standing"); *Allen v. Wenco Mgmt., LLC*, No. 1:23-CV-103, 2023 U.S. Dist. LEXIS 178605, at *8 (N.D. Ohio Sept. 29, 2023) (unpublished) ("[T]he weight of post-*TransUnion* authority establishes that [an] alleged privacy injury is sufficiently concrete for Article III purposes.") (citing *Bohnak*, 79 F.4th at 285 (2d Cir. 2023) and *Clemens v. ExecuPharm Inc*., 48 F.4th 146, 154–55 (3d Cir. 2022)); *McCreary v. Filters Fast LLC*, No. 3:20-cv-595, 2021 U.S. Dist. LEXIS 133608, at *11–12 (W.D.N.C. July 19, 2021) (unpublished) (finding an injury-in-fact when plaintiff alleged dark web exposure).

4. Emotional Injuries

Plaintiffs also suffered emotional injuries which suffice to establish injury-in-fact. Compl. ¶¶30, 42, 54, 67, 79; *Maser*, 2024 U.S. Dist. LEXIS 102196, at *20 (noting that "emotional distress" can establish Article III standing when there is "a substantial risk of future harm"); *TransUnion*, 594 U.S. at 436 n.7 (suggesting that an "emotional distress injury" could establish Article III standing when caused by the "knowledge that he or she is exposed to a risk of future [] harm"); *Bowen v. Paxton Media Grp., LLC*, No. 5:21-CV-00143, 2022 U.S. Dist. LEXIS 162083,

at *14 (W.D. Ky. Sept. 8, 2022) (unpublished) (explaining that "emotional distress related to the[] fear of identity theft" is a concrete injury). After all, "[f]or more than a century, American courts have recognized damages as a remedy for emotional distress caused by invasions of privacy and similar torts." *In re Pawn Am. Consumer Data Breach Litig*., No. 21-CV-2554, 2022 U.S. Dist. LEXIS 140107, at *10 (D. Minn. Aug. 8, 2022) (unpublished) ("emotional distress directly caused by the theft of their private information . . . is sufficient to establish standing").

5. Damage to Value of PII

Plaintiffs suffered damage to their PII via exposure in the Data Breach, theft by ALPHV BlackCat, and apparent disclosure on the dark web—which establishes Article III standing. Compl. ¶¶97–107; *Finesse Express, LLC v. Total Quality Logistics, LLC*, No. 1:20cv235, 2021 U.S. Dist. LEXIS 60648, at *7 (S.D. Ohio Mar. 30, 2021) (unpublished) (explaining that "[c]ourts have held that a loss in value of personal information supports a finding that a plaintiff has suffered an injury in fact"); *In re Marriott Int'l, Inc., Customer Data Sec. Breach Litig.,* 440 F. Supp. 3d 447, 461–62 (D. Md. 2020) (explaining that "the growing trend across courts that have considered this issue is to recognize the lost property value of this information" because "the value of consumer personal information is . . . in the economic benefit the consumer derives"); *Smallman v. MGM Resorts Int'l*, 638 F. Supp. 3d 1175, 1191 (D. Nev. 2022) (explaining that a "Data Breach devalue[s] Plaintiffs' PII by interfering with their fiscal autonomy"); *In re Experian Data Breach Litig.*, No. SACV 15-1592, 2016 U.S. Dist. LEXIS 184500, at *14 (C.D. Cal. Dec. 29, 2016) (citation omitted) (unpublished) ("[A] growing number of federal courts have now recognized Loss of Value of PII as a viable damages theory.").

6. Lost Time and Mitigation Efforts

Plaintiffs lost time attempting to mitigate the fallout of the Data Breach and such allegations are sufficient because "mitigation [] efforts" establish Article III standing when there is "a substantial risk of future harm." *Maser*, 2024 U.S. Dist. LEXIS 102196, at *20; *Gordon*, 344 F. Supp. 3d at 1241 (finding standing when plaintiff "suffered actual harm in time spent addressing the theft"); *Webb*, 72 F.4th at 377 ("We join other circuits in concluding that time spent responding to a data breach can constitute a concrete injury sufficient to confer standing[.]") (collecting cases); *Hutton v. Nat'l Bd. of Exam'rs in Optometry, Inc*., 892 F.3d 613, 622 (4th Cir. 2018) (holding that "time lost in seeking to respond to fallout from the [] data breach" establishes standing "when a substantial risk of harm actually exists"). Here, Plaintiffs lost time, *inter alia*, disputing fraud, filing a report with the Federal Trade Commission ("FTC"), researching the Data Breach, reviewing credit reports, reviewing financial accounts, changing passwords, and requesting credit freezes. Compl. ¶¶29, 41, 53, 66.

B. Injunctive Relief

Academy argues that Plaintiffs do not have standing to seek injunctive relief because they are not at imminent risk of harm. Doc. 49 at 12–13. However, as Plaintiffs have already demonstrated, they are at imminent risk of future harm as a result of the Data Breach because they have alleged their PII has seemingly been posted to the dark web by the cybercriminals who hacked Academy and at least one Plaintiff has already experienced actual misuse and fraud. *See* Compl. ¶¶65, 106. In addition, all Plaintiffs allege that their PII is still in the possession of Academy, and that Academy has not informed Class Members of how it has improved its data security (if at all). *Id.* ¶¶33, 45, 57, 69, 82, 99. It is likely that significant security enhancements are needed to fully protect Plaintiffs' PII, as ALPHV Blackcat claimed that they had been in Academy's network "for

a very long time." *Id.* ¶106. Plaintiffs' PII is still unsafe in the hands of Academy, so they require injunctive relief to ensure that Academy implements and maintains appropriate protections for PII in the future, and to help ensure Plaintiffs are not again subjected to a breach and resultant harm.

Most courts conclude that plaintiffs have standing to seek injunctive relief after a data breach. *See, e.g.*, *In re Unite Here Data Sec. Incident Litig.*, No. 24-cv-1565, 2024 U.S. Dist. LEXIS 124481, at *14 (S.D.N.Y. July 15, 2024) (unpublished) ("[B]ecause plaintiffs already face a risk of identity theft from the first data breach, plaintiffs may similarly seek lifetime credit monitoring and identity theft insurance to mitigate the risk."); *Stallone v. Farmers Grp., Inc.*, No. 2:21-cv-01659, 2022 U.S. Dist. LEXIS 188945, at *27 (D. Nev. Oct. 15, 2022) (unpublished) (collecting cases and holding that because the defendants experienced a data breach, "[p]laintiff therefore faces a 'real and immediate threat' of further disclosure of his PII, which remains in the hands of Defendants"); *Gordon*, 344 F. Supp. 3d at 1252 (holding "these allegations sufficiently show that [p]laintiffs may again be injured by a data breach, due to [d]efendant's alleged pattern of neglecting its data security systems and its alleged retention of [p]laintiffs' PII"); *In re Fortra File Transfer Software Data Sec. Breach Litig.*, No. 24-MD-03090, 2024 U.S. Dist. LEXIS 169281, at *39 (S.D. Fla. Sept. 18, 2024) (unpublished) (holding that because plaintiffs were at imminent risk of harm, they have standing to seek injunctive relief).

Academy's one cited case to the contrary does not defeat the weight of authority and the facts of this case. In that case, the plaintiffs only requested injunctive relief because their PII was still in the hands of the defendant. *See Webb*, 72 F.4th at 378. Here, in contrast, on top of alleging that injunctive relief is required to protect the PII in the hands of Academy, Plaintiffs seek injunctive relief to protect them from future fraud through extended credit monitoring. *See, e.g.*,

Compl. ¶244. While Plaintiffs' cited cases demonstrate that risk of another breach is sufficient to confer standing for injunctive relief, Plaintiffs' allegations go beyond that.

C. Rule 12(b)(6) Arguments

1. Plaintiffs Adequately Plead Their Negligence Claim

In challenging Plaintiffs' negligence claim, Academy first argues that the claim should be dismissed on the grounds that Utah does not permit damages for the risk of future harm. Doc. 49 at 13–14. While Plaintiffs do allege that they are at an imminent risk of future harm, this is not the only type of damage that Plaintiffs allege. Plaintiffs allege that they and Class Members suffered:

> (i) a substantially increased risk of identity theft and fraud—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) improper disclosure of their PII; (iii) breach of the confidentiality of their PII; (iv) deprivation of the value of their PII, for which there is a well-established national and international market; (v) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of identity theft they face and will continue to face; (vii) actual or attempted fraud; (viii) invasion of privacy; (ix) statutory damages; (x) nominal damages; and (xi) the continued increased risk to their PII.

Compl. ¶242. All Plaintiffs have spent time dealing with the Data Breach. *Id*. ¶¶29, 30, 41, 42, 53, 54, 66, 67, 78, 79. Plaintiffs allege an increase in spam communications. *Id*. ¶¶32, 44, 56, 81. Plaintiffs also allege anxiety, stress, and frustration as a result of the Data Breach. *Id*. ¶¶30, 42, 54, 67, 79. Plaintiffs also allege actual identity theft as a result of the Data Breach. *Id*. ¶65. As Plaintiffs allege *supra*, courts often find that these types of damages are compensable in data breach class actions. *See* Sec. IV.A; *Dieffenbach v. Barnes & Noble, Inc.*, 887 F.3d 826, 828 (7th Cir. 2018) (holding that mitigation efforts "can justify money damages, just as they support standing"); *Gibson v. Warrior Met Coal Inc.*, No. 7:24-cv-95, 2024 U.S. Dist. LEXIS 181017, at *15 (N.D. Ala. Oct. 3, 2024) (holding that an increase in spam calls, texts, and emails demonstrated actual misuse and damages); *In re Gallagher Data Breach Litig.*, 631 F. Supp. 3d 573, 587 (N.D. Ill.

2022) (holding that emotional harms such as anxiety are sufficient to allege actual damages). Plaintiffs' alleged damages are compensable and go beyond imminent risk of future harm.

a. Economic Loss Rule

Academy argues that Plaintiffs' negligence claims are barred by the economic loss doctrine. *See* Doc. 49 at 15. It ignores Plaintiffs' non-economic injuries, including loss of time, breach of confidentiality, and emotional distress. Compl. ¶¶30, 42, 54, 67, 79, 242; *see also In re Ambry Genetics Data Breach Litig.*, 567 F. Supp. 3d 1130, 1142 (C.D. Cal. 2021) (noting that time spent dealing with a data breach, anxiety, concern, and unease, and loss of privacy are non-economic injuries); *Alexander v. Wells Fargo Bank, N.A.*, No. 23-cv-617, 2023 U.S. Dist. LEXIS 139242, at *8 (S.D. Cal. Aug. 9, 2023) (unpublished) (time spent dealing with a data breach is a non-economic injury). In addition, Plaintiff Smith alleges actual identity theft. Compl. ¶65. Plaintiffs adequately allege several non-economic injuries that get Plaintiffs' negligence claim past the economic loss rule.

However, even if Plaintiffs only alleged economic injuries, their claims should still proceed. As Academy notes, Utah courts apply the economic loss rule only when a party has no independent duty to perform a specific action outside of a contract. *See* Doc. 49 at 15 (quoting *Reighard v. Yates*, 2012 UT 45, ¶21). Plaintiffs' home states either do not apply the economic loss rule to non-products liability claims or have this same exception or a similar applicable exception. *See Tiara Condo. Ass'n v. Marsh & McLennan Cos.*, 110 So. 3d 399, 407 (Fla. 2013) ("[T]he economic loss rule applies only in the products liability context."); *Eastwood v. Horse Harbor Found., Inc.*, 241 P.3d 1256, 1264 (Wash. 2010) (discussing the independent duty exception); *Taylor v. Taylor*, 422 P.3d 1116, 1125 (Idaho 2018) (noting an exception exists "where unique circumstances require a reallocation of the risk"); *Peeples v. Caroline Container, LLC*, No. 4:19-

CV-00021, 2019 U.S. Dist. LEXIS 238313, at *11 (N.D. Ga. Apr. 4, 2019) (discussing independent duty exception under Georgia law). Plaintiffs allege that Academy had a general duty to protect Plaintiffs' PII that did not arise out of contract. Compl. ¶231. Plaintiffs also allege that Academy's duties arose from statute, including Section 5 of the Federal Trade Commission Act and the Gramm-Leach-Bliley Act. *Id.* ¶¶232–33.

Plaintiffs allege both non-economic injuries and duties outside of contract. Accordingly, the economic loss rule does not apply to Plaintiffs' negligence claim.

b. Duty and Breach

Academy also challenges that Plaintiffs have not alleged that Academy had a duty to protect their PII. *See* Doc. 49 at 16–17. Not so. Plaintiffs allege that, among other duties, Academy had a duty to adequately protect PII by implementing adequate security practices and procedures. *See, e.g.*, Compl. ¶¶134–135. Plaintiffs even allege that Academy acknowledged its duty in its Privacy Policy. *See id*. ¶¶92–93.

Academy next argues that it has no duty to protect against criminal acts from third parties. *See* Doc. 49 at 16. However, Academy admits that entities have a duty to protect against criminal acts by a third party when "the business owner knows, or should know, that criminal acts are likely to occur." *Id*. (quoting *Steffensen v. Smith's Mgmt. Corp.*, 862 P.2d 1342, 1344–45 (Utah 1993)); *Ga. CVS Pharmacy, LLC v. Carmichael*, 890 S.E.2d 209, 222 (Ga. 2023) (same under Georgia law); *McCain v. Fla. Power Corp.*, 593 So. 2d 500, 503 (Fla. 1992) (duty to protect against "*foreseeable zone of risk*") (emphasis in original) (citation omitted); *Lauritzen v. Lauritzen*, 874 P.2d 861, 866 (Wash. Ct. App. 1994) (discussing special relationship exception to absence of third-party liability and noting one such relationship can be business owner and customers); *Henrie v. Corp. of the President of the Church of Jesus Christ Latter-Day Saints*, 395 P.3d 824, 829 (Idaho

2017) (noting a person has a duty to protect others against harm where there is foreseeable risk and the person has the right and ability to control the third-party's conduct). Plaintiffs allege exactly that, stating, "Defendant knew or should have known that the PII that they collected and maintained would be targeted by criminals." Compl. ¶148. Plaintiffs cite numerous sources demonstrating that cybercriminals target the sensitive PII that Academy stored. *See id*. ¶¶140–50. Even the case that Academy heavily relies on holds that businesses have a duty to protect against data breaches. *See In re Waste Mgmt. Data Breach Litig.*, No. 21cv6147, 2022 U.S. Dist. LEXIS 32798, at *11–12 (S.D.N.Y. Feb. 24, 2022) (unpublished) ("*In re Waste Management*") (noting that while a business does not have a duty to protect against unforeseeable third-party criminal acts, "a duty is still appropriate here because attempts by hackers to access PII stored in an internal network are highly foreseeable"). Accordingly, Plaintiffs adequately allege that Academy had a duty to protect PII but failed to do so.

Academy claims Plaintiffs have not adequately alleged a breach of duty, stating "Plaintiffs have not sufficiently alleged the absence of reasonable conduct." Doc. 49 at 16. Academy cites *In re Waste Management* for support (*see id*.), but there the court noted that the complaint did not have any specific allegations regarding the defendant's failure to protect the PII in that case. *See* 2022 U.S. Dist. LEXIS 32798, at *12. Academy contends the same deficiency in Plaintiffs' Complaint, arguing that "not once do Plaintiffs say specifically what concrete measure" Academy could have taken to prevent the Data Breach. Doc. 49 at 17. However, Plaintiffs dedicated 26 paragraphs of the Complaint to detailing the statutory and industry standards that Academy failed to follow. *See* Compl. ¶¶108–33. Specifically, Plaintiffs allege, *inter alia*, Academy failed to "properly implement basic data security practices," "failed to provide annual privacy notices to consumers after the relationship ended," and failed to meet certain specific industry standards,

including the NIST Cybersecurity Framework Version 1.1 and the Center for Internet Security's Critical Security Controls. *See id*. ¶¶115, 123, 132. Plaintiffs have adequately alleged that Academy breached its duty to protect Plaintiffs' and Class Members' PII.

2. Plaintiffs Adequately Plead Their Implied Contract Claim

Academy argues Plaintiffs failed to state a claim for breach of implied contract, asserting that Plaintiffs did not allege any material terms or conditions sufficient to establish their claim. Academy further contends that the mere act of Plaintiffs providing their PII to Academy is insufficient to constitute the meeting of the minds required to form an implied contract. However, courts infer a meeting of the minds from the mandatory submission of PII, and the terms of an implied contract are a question of fact.

A contract implied in fact requires "a manifestation of mutual assent, by words or actions or both, which reasonably are interpretable as indicating an intention to make a bargain with certain terms or terms which reasonably may be made certain." *Lopez v. Admin. Off. of Cts.*, 719 F.3d 1178, 1182 (10th Cir. 2013) (quoting *Heideman v. Washington City*, 155 P.3d 900, 908 (Utah App. 2007)). The elements under Florida, Washington, Idaho, and Georgia law are substantially similar. *See, e.g.*, *Fertilizantes Tocantins S.A. v. TGO Agric. (USA), Inc.,* 599 F. Supp. 3d 1193, 1205 (M.D. Fla. 2022) (Florida law); *Heaton v. Imus*, 608 P.2d 631, 632 (Wash. 1980) (Washington law); *Clements v. Jungert*, 408 P.2d 810, 815 (Idaho 1965) (Idaho law); *Dawes Mining Co. v. Callahan*, 267 S.E.2d 830, 832 (Ga. Ct. App. 1980) (Georgia law).

A person who is required to provide sensitive PII reasonably expects that the party they are turning it over to will safeguard that information. Various courts nationwide have recognized this, in the context of both consumers and employees. *See, e.g.*, *In re Arby's Rest. Grp. Inc. Litig.*, No. 1:17-CV-0514, 2018 U.S. Dist. LEXIS 131140, at *55–58 (N.D. Ga. Mar. 5, 2018) (unpublished)

(reasonable to infer the defendant and consumer plaintiffs had an understanding that defendant must protect the PII provided to it); *In re Target Corp. Customer Data Sec. Breach Litig.*, 66 F. Supp. 3d 1154, 1161 (D. Minn. 2014) (allegations that an implied contract was formed when plaintiffs agreed to pay for products with debit or credit cards at stores and the defendant agreed to safeguard the PII were sufficient to proceed past motion to dismiss); *In re Michaels Stores Pin Pad Litig.*, 830 F. Supp. 2d 518, 531 (N.D. Ill. 2011) (same); *Anderson v. Hannaford Bros. Co.*, 659 F.3d 151, 159 (1st Cir. 2011) (stating, "a customer does not expect—and certainly does not intend—the merchant to allow unauthorized third-parties to access that data"); *Smallman*, 638 F. Supp. 3d at 1195 (plaintiffs stated a claim for implied contract where they alleged they were required to provide their PII to the defendant as a condition of staying at defendant's hotel, and understood that defendant would protect their PII); *Farmer v. Humana, Inc*., 582 F. Supp. 3d 1176, 1187 (M.D. Fla. 2022) (plaintiff had stated a claim for implied contract where they alleged they were required to provide their personal information to the defendant as a condition of obtaining health insurance); *Medoff v. Minka Lighting, LLC*, No. 2:22-CV-08885, 2023 U.S. Dist. LEXIS 81398, at *25–29 (C.D. Cal. May 8, 2023) (unpublished) (denying employer defendant's motion to dismiss implied contract claim where the plaintiff alleged they provided PII to defendant in exchange for employment).

In fact, as one court put it: "it is difficult to imagine how, in our day and age of data and identity theft, the mandatory receipt of . . . sensitive personal information would not imply the recipient's assent to protect the information sufficiently." *Castillo v. Seagate Tech., LLC*, No. 16-cv-01958, 2016 U.S. Dist. LEXIS 187428, at *29 (N.D. Cal. Sept. 14, 2016) (unpublished).

Plaintiffs have sufficiently alleged that an implied contract was formed when they and Class Members agreed to provide money and their PII to Academy, and Academy agreed to

provide mortgage services and to safeguard their PII. For instance, Plaintiffs allege "[i]n collecting and maintaining PII, Academy implicitly agreed that it will safeguard the data using reasonable means according to its internal policies, as well as state and federal law," and that Academy promised in its Privacy Policy, to "use commercially reasonable efforts to protect [customers'] personal information . . . from access, loss, misuse, alteration, or destruction by any unauthorized party." *Id*. ¶¶91–92.

Because Plaintiffs also allege that "Academy requires customers and employees to provide their highly sensitive personally identifiable information to facilitate its mortgage services," they have sufficiently pleaded there was an implied contract where individuals who wished to utilize Academy's mortgage services would be required to provide their PII, which Academy would in turn protected from "access, loss, misuse, alteration, or destruction by any unauthorized party." *Id*. ¶¶90, 92.

Academy attempts to support its position by referencing cases that held that the submission of PII, without more, is insufficient to establish an implied contract. However, those cases make clear that the pleadings at issue were insufficient because they were "without accompanying factual allegations to show mutual assent" to protect PII. *See, e.g.*, *Tate v. EyeMed Vision Care, LLC*, No. 1:21-CV-36, 2023 U.S. Dist. LEXIS 175840, at *24–25 (S.D. Ohio Sept. 29, 2023) (unpublished) (dismissing implied contract claim because all plaintiff had alleged was a conclusory, threadbare statement that the defendant agreed to safeguard her PII); *Weekes v. Cohen Cleary P.C.*, No. CV 23-10817, 2024 U.S. Dist. LEXIS 47673, at *10–12 (D. Mass. Mar. 15, 2024) (unpublished) (same). Further, in *In re Am. Med. Collection Agency, Inc. Customer Data Sec. Breach Litig*., No. CV 19-MD-2904, 2021 U.S. Dist. LEXIS 240360 (D.N.J. Dec. 16, 2021) (unpublished), although the court dismissed the plaintiff's claim due to her statements being

conclusory, it acknowledged that in circumstances where "plaintiffs pled [] the defendants 'through privacy policies, codes of conduct, company security practices, and other conduct, implicitly promised to safeguard'" PII, courts have denied motions to dismiss implied contract claims. *Id*. at *68–73. This is precisely one of those cases. Plaintiffs have alleged that they provided their PII with the expectation that it would be protected by Academy, who promised in its Privacy Policy to safeguard their PII.

Finally, the terms of an implied contract and whether or not one exists are fact-intensive questions for the trier of fact. *See Soundvision Techs., LLC v. Templeton Grp. Ltd.*, 929 F. Supp. 2d 1174, 1189 (D. Utah 2013) (holding the existence of an implied contract is typically a question of fact that hinges on the objective manifestations of the parties' intent, making it inappropriate for resolution at the motion to dismiss stage.); *In re Target*, 66 F. Supp. 3d at 1176–77 (stating, "a determination of the terms of the alleged implied contract is a factual question that a jury must determine."); *Anderson*, 659 F.3d at 159 ("The existence of such an implied contract term is determined by the jury, which considers whether the term is indispensable to effectuate the intention of the parties."). Plaintiffs' allegations suffice to state a claim of implied contract, and the Court should deny Academy's motion as to this claim.

3. Plaintiffs Adequately Plead Their Unjust Enrichment Claim

Academy argues that Plaintiffs failed to state a cause of action for unjust enrichment because Plaintiffs did not allege how Academy benefitted from receiving their PII. However, Plaintiffs allege facts demonstrating that Academy benefitted from obtaining the PII of Plaintiffs.

To establish a claim for unjust enrichment, a plaintiff must plead facts that, if taken as true, establish three elements: "(1) a benefit conferred . . . ; (2) an appreciation or knowledge by the conferee of the benefit; and (3) the acceptance or retention [of the benefit] by the conferee . . .

under such circumstances as to make it inequitable for the conferee to retain the benefit without payment of its value." *U.S. Fid. v. U.S. Sports Specialty*, 270 P.3d 464, 468 (Utah 2012). The requirements for unjust enrichment are substantially similar under Florida, Washington, Idaho, and Georgia law. *See, e.g.*, *Hillman Const. Corp. v. Wainer*, 636 So. 2d 576, 577 (Fla. Dist. Ct. App. 1994) (Florida law); *Young v. Young*, 191 P.3d 1258, 1262 (Wash. 2008) (Washington law); *Teton Peaks Inv. Co., v. Ohme*, 195 P.3d 1207, 1211 (Idaho 2008) (Idaho law); *Wachovia Ins. Servs., Inc. v. Fallon*, 682 S.E.2d 657, 665 (Ga. 2009) (Georgia law).

Plaintiffs allege Academy required them to provide PII as a necessary component of obtaining mortgage services and/or as a condition of employment. Compl. ¶90. The PII was an essential part of Academy's business operations, without which Academy could not effectively offer or complete mortgage transactions or employ individuals to engage in business.

The very nature of mortgage services requires Academy to collect and store sensitive information, and Plaintiffs provided their PII with the expectation Academy would protect it with adequate data security. *Id*. ¶190. Retaining the benefit of Plaintiffs' mortgage payments without fulfilling the expectation of data security, which was inherent in the provision of services, makes Academy's retention of the benefit unjust. Many courts reviewing data breach cases have acknowledged this concept. *See, e.g.*, *Resnick v. AvMed, Inc*., 693 F.3d 1317, 1328 (11th Cir. 2012) (plaintiffs' allegations that defendant accepted the benefit of monies paid by plaintiffs, yet failed to adequately protect their personal information was sufficient for pleading unjust enrichment); *In re Cap. One Consumer Data Sec. Breach Litig.*, 488 F. Supp. 3d 374, 412 (E.D. Va. 2020) (same); *Fox v. Iowa Health Sys.*, 399 F. Supp. 3d 780, 802 (W.D. Wis. 2019) (same); *In re Premera Blue Cross Customer Data Sec. Breach Litig.*, 198 F. Supp. 3d 1183, 1201 (D. Or. 2016) (same); *Rudolph v. Hudson's Bay Co*., No. 18-CV-8472, 2019 U.S. Dist. LEXIS 77665, at *35–39

(S.D.N.Y. May 7, 2019) (unpublished) (denying motion to dismiss where plaintiff alleged that defendants benefitted from her use of a debit card, and wrongfully retained the benefits of that transaction despite failing to secure her data). Additionally, in data breach cases a benefit can be conferred simply by providing PII in exchange for services—Plaintiffs do not need to allege independent financial gain specifically from retaining the PII itself. *In re Cap. One*, 488 F. Supp. 3d at 413.

Regarding Plaintiff Thompson, the exchange of labor and PII in conjunction with employment also demonstrates a benefit that was conferred to Academy. *See Sackin v. TransPerfect Glob., Inc*., 278 F. Supp. 3d 739 (S.D.N.Y. 2017) (former employees could bring a claim of unjust enrichment against a company who did not sufficiently protect their PII because the company received the benefits of the former employees' labor, and "was enriched at Plaintiffs' expense when it chose to cut costs by not implementing security measures to protect Plaintiffs' PII which Defendant required or obtained in the course of Plaintiffs' employment").

Despite Academy's contentions, this case is inapposite to *Tate*, 2023 U.S. Dist. LEXIS 175840, and *Gordon*, 344 F. Supp. 3d at 1249, where the transaction was a "traditional exchange of payment for goods and services." *Tate*, 2023 U.S. Dist. LEXIS 175840 at *25. Further, although Academy cites *In re Target* to support its position, the *In re Target* court refused to dismiss the plaintiffs' unjust enrichment claim under the theory that they would not have shopped at Target had they known of its inadequate data security practices. Plaintiffs have also made precisely such allegations here. *See* Compl. ¶¶24, 37, 49, 61; *In re Target*, 66 F. Supp. 3d at 1178. Plaintiffs adequately pleaded unjust enrichment and the motion to dismiss this claim should be denied.

4. Plaintiffs Adequately Plead Their Invasion of Privacy Claim

Academy seeks dismissal of Plaintiffs' invasion of privacy claim on two grounds: (1) that Plaintiffs failed to plead intentional interference with their private affairs that would be considered highly offensive, and (2) that Plaintiffs failed to allege anyone has viewed their PII. Both arguments lack merit.

The elements for a "public disclosure of private facts" invasion of privacy claim, as alleged in the Complaint, are: "(1) the disclosure of the private facts must be a public disclosure and not a private one; (2) the facts disclosed to the public must be private facts, and not public ones; and (3) the matter made public must be one that would be highly offensive and objectionable to a reasonable person of ordinary sensibilities." *Shattuck-Owen v. Snowbird Corp,* 16 P.3d 555, 558 (Utah 2000) (quoting *Stein v. Marriott Ownership Resorts, Inc*., 944 P.2d 374, 380 (Utah Ct. App. 1997)); *see also Cape Publ'ns, Inc. v. Hitchner*, 549 So. 2d 1374, 1377 (Fla. 1989) (Florida law); *White v. Town of Winthrop*, 116 P.3d 1034, 1037 (Wash. Ct. App. 2005) (Washington law); *Berian v. Berberian*, 483 P.3d 937, 949 (Idaho 2020) (Idaho law); *Eason v. Marine Terminals Corp*., 710 S.E.2d 867, 871 (Ga. Ct. App. 2011) (Georgia law).

Various courts have held that allegations of a defendant's disclosure of PII in data breach cases constitute a valid claim for invasion of privacy by public disclosure of a plaintiff's private facts. *See, e.g.*, *In re Ambry*, 567 F. Supp. 3d at 1143 (refusing to dismiss invasion of privacy claim at motion to dismiss stage); *In re USAA Data Sec. Litig*., 621 F. Supp. 3d 454, 466 (S.D.N.Y. 2022) (same); *Shedd v. Sturdy Mem'l Hosp., Inc*., No. 2173-cv-00498C, 2022 Mass. Super. LEXIS 7, at *32 (Mass. Super. Apr. 5, 2022) (unpublished) (denying a motion to dismiss an invasion of privacy claim where the defendant's inadequate security measures allowed unauthorized persons to access plaintiffs' personal information during a ransomware attack).

Although the determination of whether a disclosure is "highly offensive" is typically a question for the jury, *see Stein*, 944 P.2d at 379, some courts have held that the disclosure of PII in data breach cases would necessarily be offensive to a reasonable person because it would make a victim a "ready target[ ] for targeted phishing and extortion attacks." *Baton v. Ledger SAS*, No. 21-CV-02470, 2024 U.S. Dist. LEXIS 125342, at *29 (N.D. Cal. July 16, 2024) (unpublished).

Here, Plaintiffs have sufficiently pled the first two elements of an invasion of privacy claim by alleging Academy's failure to maintain adequate security measures resulted in the public disclosure of their PII. Specifically, Plaintiffs assert Academy's inadequate data security allowed unauthorized third parties to access their PII, and as a direct consequence, their PII is now available on the dark web. Compl. ¶¶26, 101–102, 105–106, 274. Plaintiffs have also alleged that the public disclosure of their PII would be highly offensive to a reasonable person, and that Academy's failure to safeguard their PII has made them a ready target for fraud. *Id*. ¶¶162–190, 273.

For the reasons set forth above, Plaintiffs' allegations are sufficient to state a claim of invasion of privacy, and this Court should therefore deny Academy's motion to dismiss this claim.

5. Plaintiffs Adequately Plead Violations of the Washington Consumer Protection Act ("WCPA")

Academy also challenges Plaintiffs' claim under the WCPA. Doc. 49 at 22. However, courts regularly find that a failure to implement reasonable data security suffices to demonstrate an injury under the WCPA. *See Veridian Credit Union v. Eddie Bauer, LLC*, 295 F. Supp. 3d 1140, 1162 (W.D. Wash. 2017) (denying motion to dismiss and finding that the defendant's alleged failure "to take proper measures to protect account information" and "failure to employ adequate data security measures" caused "'substantial injury' to consumers"); *Buckley v. Santander Consumer USA, Inc.*, No. C17-5813, 2018 U.S. Dist. LEXIS 53411, at *12 (W.D. Wash. Mar. 29, 2018) (unpublished) (finding that "failure to take reasonably adequate security measures

constitutes an unfair act" and denying motion to dismiss WCPA claim for this reason); *In re Mednax Servs. Inc. Customer Data Sec. Breach Litig.*, 603 F. Supp. 3d 1183, 1218 (S.D. Fla. 2022) (denying motion to dismiss WCPA claim in data breach case); *In re Cap. One*, 488 F. Supp. 3d at 428–29 (denying motion to dismiss WCPA claim).

While Academy challenges the fact that it did not offer data security services for sale, the promise to safeguard PII is inherent to any transaction in which one is required to entrust confidential information to another. *In re Marriott*, 440 F. Supp. 3d at 466 ("it is enough to allege that there was an explicit or implicit contract for data security, that plaintiffs placed value on that data security, and that Defendants failed to meet their representations about data security"). Indeed here, "the facts alleged [] permit the reasonable inference that requiring someone to provide a Social Security number and other sensitive personal information as part of a transaction carries with it the recipient's implied agreement to reasonably safeguard it." *Hall v. Centerspace, LP*, No. 22-CV-2028, 2023 U.S. Dist. LEXIS 83438, at *16 (D. Minn. May 12, 2023) (unpublished) (citing *Mackey v. Belden, Inc.*, No. 4:21-CV-00149, 2021 U.S. Dist. LEXIS 145000, at *23 (E.D. Mo. Aug. 3, 2021) (unpublished)). And to the extent Academy challenges Plaintiffs' damages under the WCPA, "[m]onetary damages need not be proved; unquantifiable damages may suffice." *Panag v. Farmers Ins. Co. of Wash.*, 204 P.3d 885, 900 (Wash. 2009). Accordingly, Academy's motion to dismiss the WCPA claim must be denied.

6. Plaintiffs Adequately Plead Violations of the Idaho Consumer Protection Act ("ICPA")

The ICPA "prohibits unfair methods of competition and unfair or deceptive acts or practices in the conduct of trade or commerce within the State of Idaho." *Pickering v. Sanchez*, 544 P.3d 135, 142 (Idaho 2024) (quoting *Litster Frost Inj. Laws., PLLC v. Idaho Inj. L. Grp., PLLC*, 518 P.3d 1, 11 (Idaho 2022)). "The ICPA is remedial legislation intended to deter unfair

and deceptive trade practices and is to be construed liberally." *In re Edwards*, 233 B.R. 461, 470 (Bankr. D. Idaho 1999). Importantly, scienter is not an element of the ICPA. *Id*. ("It is not necessary to prove actual intent to deceive or actual deception on behalf of the defendant as long as a tendency or capacity to mislead consumers has been established.").

Contrary to Academy's argument, Plaintiffs have alleged that Academy's failure to implement reasonable data security is an unfair practice, and its failure to disclose its inadequate security is a deceptive act. *See, e.g.*, *In the Matter of LabMd, Inc., A Corp*, 2016-2 Trade Cas. (Henry Ford) ¶79708, 2016 FTC LEXIS 128, at *32 (MSNET July 28, 2016) ("[T]he Commission concludes that LabMD's data security practices were unreasonable and constitute an unfair act or practice in violation of Section 5 of the FTC Act."). Moreover, an "ascertainable loss of money" under Idaho Code section 48-608(1) is, amongst other things, "[a]ny deprivation" of money that "is capable of being discovered, observed, or established." *Litster*, 518 P.3d at 13 (quoting IDAPA 04.02.01.020.05). Here Plaintiffs have lost the value of their time and suffered from the diminished value of their PII, which are a quantifiable loss. Simply put, Plaintiffs need not allege out of pocket losses to sustain their ICPA claim.

CONCLUSION

For the foregoing reasons, Plaintiffs respectfully request that the Court deny Academy's Motion to Dismiss in its entirety. To the extent the Court dismisses any claim without prejudice, Plaintiffs request leave to amend the Complaint. *Strand v. USANA Health Scis., Inc*., No. 2:17-cv-00925, 2020 U.S. Dist. LEXIS 119007, at *3 (D. Utah July 6, 2020) (granting leave to amend in view of "liberal standard for allowing leave to amend pleadings").

Dated: October 7, 2024

Respectfully submitted,

/s/ Brittany Resch

Brittany Resch*
Raina C. Borrelli*
STRAUSS BORRELLI PLLC
980 N. Michigan Ave. Suite 1610
Chicago, IL, 60611
Telephone: (872) 263-1100
Facsimile: (872) 263-1109
bresch@straussborrelli.com
raina@straussborrelli.com

Andrew W. Ferich*
AHDOOT & WOLFSON, PC
201 King of Prussia Road, Suite 650
Radnor, PA 19087
Telephone: (310) 474-9111
Facsimile: (310) 474-8585
aferich@ahdootwolfson.com

Anthony L. Parkhill*
BARNOW AND ASSOCIATES, P.C.
205 West Randolph Street, Ste. 1630
Chicago, IL 60606
Telephone: (312) 621-2000
Facsimile: (312)641-5504
aparkhill@barnowlaw.com

Nickolas J. Hagman**
CAFFERTY CLOBES MERIWETHER & SPRENGEL LLP
135 S. LaSalle, Suite 3210
Chicago, Illinois 60603
Telephone: (312) 782-4880
Facsimile: (312) 782-4485
nhagman@caffertyclobes.com

James E. Magleby (7247)
Jennifer Fraser Parrish (11207)
MAGLEBY CATAXINOS & GREENWOOD, PC
141 West Pierpont Avenue
Salt Lake City, Utah 84101
Telephone: (801) 359-9000

Facsimile: (801) 359-9011
magleby@mcg.law
parrish@mcg.law

Jason R. Hull [11202]
Trevor C. Lang [14232]
MARSHALL OLSON & HULL, PC
Newhouse Building
Ten Exchange Place, Suite 350
Salt Lake City, Utah 84111
Telephone: (801) 456-7655
jhull@mohtrail.com
tlang@mohtrial.com

Counsel for Plaintiffs and the Class

* admitted *pro hac vice*
** *pro hac vice* pending or to be submitted

CERTIFICATE OF SERVICE

I, Brittany Resch, hereby certify that I electronically filed the foregoing with the Clerk of the Court using the CM/ECF system, which will send notification of such filing to counsel of record via the ECF system.

DATED this 7th day of October, 2024.

STRAUSS BORRELLI PLLC

By: */s/ Brittany Resch*

Brittany Resch
STRAUSS BORRELLI PLLC
One Magnificent Mile
980 N Michigan Avenue, Suite 1610
Chicago IL, 60611
Telephone: (872) 263-1100
Facsimile: (872) 263-1109
bresch@straussborrelli.com